Listing of Claims

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of messages that were sent over a data network;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown network attack; and

sending the common content to one or more of a signature blocker and a signature manager for use as a new signature in identifying the previously unknown intrusive network attack.

2. (Previously Presented) A method as in claim 1, wherein said analyzing comprises determining frequently occurring sections of message information.

3. (Previously Presented) A method as in claim 1, wherein said analyzing comprises determining that increasing number of sources and destinations are sending and/or receiving data.

4. (Previously Presented) A method as in claim 1, further comprising analyzing for the presence of a specified type of code within said collection of data.

5. (Previously Presented) A method as in claim 2, further comprising, after said analyzing determines said frequently occurring sections of message information, carrying out an additional test on said frequently occurring sections of message information.

6. (Previously Presented) A method as in claim 5, wherein said carrying out the additional test comprises looking for an increasing number of at least one of sources and destinations of said frequently occurring sections of message information.

7. (Previously Presented) A method as in claim 5, wherein said carrying out the additional test comprises looking for code within the frequently occurring sections.

8. (Previously Presented) A method as in claim 1, wherein said reducing said data items comprises carrying out a hash function on said data items.

9. (Previously Presented) A method as in claim 2, wherein said determining frequently occurring sections comprises:

using at least first, second, and third data reduction techniques on each said data item to obtain at least first, second and third reduced data items;

counting said first, second, and third reduced data items; and

establishing said frequently occurring sections when all of said at least first, second, and third reduced data items have a frequency of occurrence greater than a specified amount.

10. (Previously Presented) A method as in claim 1, wherein said collection of data items comprises a portion of the network payload.

11. (Previously Presented) A method as in claim 5, wherein said carrying out the additional test comprises:

maintaining a first list of unassigned addresses;

forming a second list of sources that have sent to addresses on said first list; and

comparing a current source of a frequently occurring section to said second list.

12. (Previously Presented) A method as in claim 11, wherein said carrying out the additional test comprises reducing addresses in said first list and said second list to reduced addresses, wherein the reduced addresses have a smaller size and a constant predetermined relation with the addresses and at least some of the addresses that differ are reduced to the same reduced address.

13. (Previously Presented) A method as in claim 5, wherein said carrying out the additional test comprises:

first monitoring a first content sent to a destination;

second monitoring a second content sent by said destination; and

determining a correlation between said first content and said second content.

14. (Previously Presented) A method as in claim 13, wherein:

said first monitoring comprises monitoring multiple destinations; and

said second monitoring comprises monitoring multiple destinations during a different time period than said first monitoring.

15. (Previously Presented) A method as in claim 14, wherein said first and second monitoring comprises:

reducing information about said destinations; and

storing at least one table about said data reduced information.

16. (Previously Presented) A method as in claim 10, wherein said collection of data items further comprises a portion of a network header.

17. (Previously Presented) A method as in claim 11, wherein said portion of a network header comprises a port number indicating a service requested by a network packet.

18. (Previously Presented) A method as in claim 17, wherein said port number comprises a source port or a destination port.

19. (Previously Presented) A method as in claim 1, wherein:

said data items comprise a first subset of a network packet including payload and header; and

the method further comprises obtaining a second subset of the same network packet for subsequent analysis.

20. (Previously Presented) A method as in claim 1, further comprising forming a plurality of data items from each of a collection of network packets, each of said plurality of data items comprising a specified subset of the network packets.

21. (Previously Presented) A method as in claim 1, further comprising forming a plurality of data items from each of a collection of network packets, each of said plurality of data items comprising a continuous portion of payload and information indicative of a port number indicating a service requested by the network packet.

22. (Previously Presented) A method as in claim 2, wherein said reducing said data items and said determining frequently occurring sections comprises:

taking a first hash function of said data items;

first maintaining a first counter, with a plurality of stages, and incrementing one of said stages based on an output of said first hash function;

taking a second hash function of said data items; and

second maintaining a second counter, with a plurality of stages, and incrementing one of said stages of said second counter based on an output of said second hash function.

23. (Previously Presented) A method as in claim 22, further comprising:

checking said one of said stages of said first counter and said one of said stages of said second counter against a threshold; and

identifying a first reduced data item as associated with frequently occurring content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold.

24. (Previously Presented) A method as in claim 23, further comprising adding the first reduced data item to a frequent content buffer table.

25. (Previously Presented) A method as in claim 24, further comprising:

taking at least a third hash function of said data items; and

incrementing a stage of at least a third counter based on said third hash function,

where said identifying said first reduced data item as associated with frequently occurring content only when all of said stages of each of said first, second, and third counters are each above said threshold.

26. (Previously Presented) A method as in claim 22, further comprising:

obtaining said data items by taking a first part of messages; and

subsequently obtaining new data items by taking a second part of the messages.

27. (Previously Presented) A method as in claim 26, wherein at least one of said hash functions comprises an incremental hash function.

28. (Previously Presented) A method as in claim 3, wherein reducing said data items comprises:

hashing at least one of the source or destination addresses to form a collection of hash values;

first determining a unique number of said hash values; and

second determining a number of said one of source or destination addresses based on said first determining.

29. (Previously Presented) A method as in claim 28, further comprising scaling the hash values prior to said second determining.

30. (Previously Presented) A method as in claim 29, wherein said scaling comprises:

scaling by a first value during a first counting session ; and

scaling by a second value during a second measurement session.

31. (Previously Presented) A method as in claim 7, wherein said detecting code comprises:

looking for a first valid opcode at a first location;

based on said first valid opcode, determining a second location representing an offset to said first valid opcode; and

looking for a second valid opcode at said second location.

32. (Previously Presented) A method as in claim 31, further comprising establishing that a first section includes code when a predetermined number of valid opcodes are found at proper distances.

33. (Previously Presented) A method as in claim 1, further comprising:

determining a list of first computers that are susceptible to a specified attack; and

monitoring only messages directed to said first computers for said specified attack.

34. (Previously Presented) The method of claim 33, where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable as said specified attack.

35. (Original) A method as in claim 34, wherein said checking comprises checking for a field that is longer than a specified length.

Claims 36.-68. (Canceled)

69. (Previously Presented) A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

monitoring network content on a network and obtaining at least portions of the data on said network;

data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion;

analyzing said reduced data portions to find network content which repeats a specified number of times in order to establish said network content which repeats said specified number of times as frequent content;

identifying address information of said frequent content, wherein the address information includes at least one of source information or destination information that characterizes the respective of sources and/or destinations of said frequent content and determining if a number of sources and/or destinations of said frequent content is increasing;

identifying the frequent content as associated with the previously unknown network attack based on said identifying and determining, and

sending the frequent content to one or more of a signature blocker and a signature manager.

70. (Previously Presented) A method as in claim 69, wherein said monitoring network content comprises obtaining both portions of the data on the network and portnumbers indicating services requested by network packets.

71. (Previously Presented) A method as in claim 70, wherein said obtaining portions of the network data comprises:

defining a window which samples a first portion of network data at a first time in accordance with a position of the window; and

sliding said window to a second position at a second time which samples a second portion of said network data, wherein said second position has a specified offset from the first portion.

72. (Previously Presented) A method as in claim 71, wherein said data reduction function comprises a hash function.

73. (Previously Presented) A method as in claim 72, wherein said data reduction function comprises an incremental hash function.

74. (Previously Presented) A method as in claim 69, wherein data reducing said portions comprises using said data reduction function in a scalable configuration.

75. (Previously Presented) A method as in claim 69, wherein said identifying comprises:

second data reducing said address information using a data reduction function; and

maintaining a table of data reduced address information.

76. (Original) A method as in claim 75, wherein said second data reducing comprises hashing said address information.

77. (Previously Presented) A method as in claim 69, further comprising testing contents of the frequent content to determine the presence of code in said frequent content.

78. (Previously Presented) A method as in claim 77, wherein said testing contents comprises:

identifying an opcode in said frequent content;

determining a length of the opcode ; and

looking for another opcode at a location within said frequent content based on said length.

79. (Previously Presented) A method as in claim 69, further comprising monitoring for scanning of addresses.

Claims 80.-87. (Canceled)

88. (Previously Presented) A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the previously unknown network attack;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack;

carrying out an additional test on said frequently occurring sections of message information, comprising

maintaining a first list of unassigned addresses, wherein the unassigned addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address,

forming a second list of source addresses that have sent to the unassigned addresses on said first list, wherein the source addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the source addresses and at least some of the source addresses that differ are reduced to the same reduced address, and

comparing a current source of a frequently occurring section to said second list; and

based on the additional test, sending some of the frequently occurring sections to one or more of a signature blocker and a signature manager.

89. (Previously Presented) A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items comprise a first subset of a network packet including payload and header;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to detect common elements, said analyzing reviewing for common content indicative of a network attack;

obtaining a second subset of the same network packet for subsequent analysis; and

based on the subsequent analysis, sending some of the common content to one or more of a signature blocker and a signature manager.

90. (Previously Presented) The method of claim 1, wherein obtaining the collection of data items comprising obtaining the collection at a vantage link that includes a router.

91. (Previously Presented) The method of claim 69, wherein monitoring the network content comprises monitoring the network content at a vantage link that includes a router.